图书情报工作
第65卷 第22期 2021年11月



# 《数据安全法》与《档案法》协调研究

■ 王玉珏[1] 吴一诺[1,2] 凌敏菡[1]
[1] 武汉大学信息管理学院 武汉 430072 [2] 武汉大学图书情报国家级实验教学示范中心 武汉 430072

摘 要：[目的/意义] 剖析《数据安全法》与《档案法》在规制对象、立法目的以及立法原则等方面的各自偏重和相互交叉，探讨推动两部法律协调发展的必要性和可循路径，为档案与数据后续立法提供参考。[方法/过程] 通过文献调研和比较分析，提出《数据安全法》与《档案法》两部法律协调推进过程中面临的问题，通过域外经验借鉴，对两部法律配套下位法的制定提出建议。[结果/结论] 研究发现，两部法律从各自的管理实践出发，在档案与数据保护相关规定、档案与数据分级分类标准、档案与数据跨境流动等方面的法律规制协调性不足，导致部分数据陷入"灰色地带"，数据安全无从保证。文章提出：应明确档案部门在数据治理中的参与；从数据长期保存的连贯性出发建立符合我国实际的数据与档案分级标准；档案部门与数据部门协同建立重要数据跨境流动的法律法规和管理机制；完善两部法律中有关个人隐私保护的内容。

关键词：《数据安全法》 《档案法》 数据安全 档案立法 数据立法
分类号：G271
DOI：10.13266/j.issn.0252-3116.2021.22.003



## 1 引言

2020年6月18日，十三届全国人大常委会第十九次会议通过修订后的《中华人民共和国档案法》(以下简称《档案法》)，自2021年1月1日起施行。《档案法》从档案收集、整理、保护、利用、监督等各个环节健全完善了档案管理制度，并专门增设"档案信息化建设"一章，对大数据时代档案工作面临的新情况、新问题予以明确。随后，2020年7月3日，《中华人民共和国数据安全法(草案)》(以下简称《数据安全法(草案)》)向社会公开征求意见，我国第一部专门针对数据安全领域的立法正式启动。经过三次审议与修改，2021年6月10日，十三届全国人大常委会第二十九次会议通过《中华人民共和国数据安全法》(以下简称《数据安全法》)，并于2021年9月1日起施行。

早在2017年，习近平总书记便提出要切实保障国家数据安全，要加强政策、监管、法律的统筹协调，加快法规制度建设[1]。《数据安全法(草案)》公布之初，翟志勇[2]、张猛[3]、刘桂锋[4]、马忠法[5]、徐玖玖[6]等诸多学者便探讨了《中华人民共和国国家安全法》《中华人民共和国网络安全法》(以下简称《网络安全法》)《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)等法律与《数据安全法》之间的协调关系。

随着大数据、云计算、云存储、物联网等新兴技术在数字档案馆建设、政府信息开放、档案智慧服务中的应用，"档案数据化"研究成为面向人工智能时代的档案信息化建设新范式[7]。档案界逐渐认识到数据治理成为大数据时代档案管理的新视角和新职能[8]，并提出"档案领域数据本体"[9]"记录因子"[7]等新概念。同时，"档案是否属于数据""《数据安全法》与《档案法》有何关联""《数据安全法》对档案学理论及管理实践有何影响"等问题也引起司法界及图书情报界的共同关注。

华东政法大学高富平教授在2020年7月举办的《数据安全法(草案)》暨数据法治研讨会上提出为了实现对内对外双重目标，应协调和衔接《数据安全法》和《网络安全法》《档案法》等法律在数据安全方面的制度措施[10]；邓灵斌提出《数据安全法》的发布，为我国图书情报界的数据安全提供了有力法律保障[11]；金波等提出建立健全档案数据法规体系是确保档案数据安全的重要手段[12]；耿志杰等提出加

作者简介：王玉珏，副教授，博士，硕士生导师，E-mail：Yujue.wang@whu.edu.cn；吴一诺，硕士研究生；凌敏菡，硕士研究生。
收稿日期：2021-05-20 修回日期：2021-09-01 本文起止页码：24-34 本文责任编辑：杜杏叶

快新修订《档案法》与《数据安全法》《中华人民共和国保守国家秘密法》《网络安全法》等法律法规的立法衔接，制定档案数据互联网传输出境的管理条例[13]；丁家友等结合总体国家安全观、《档案法》《数据安全法》，探讨了新时代背景下档案数据安全面临的新挑战[14]。

数据处理与档案管理分别处于数据管理活动中的前后端，既在管理对象上存在交叉，又在管理环节上互为补充，共同致力于保护数据安全。而目前，《数据安全法》与《档案法》缺乏对宏观数据治理的关注，在数据安全保护、数据的分级分类、重要数据跨境流动、个人隐私保护等方面尚需磨合、协调。因此，探讨《数据安全法》与《档案法》协调发展的现存问题，对贯彻落实既有法律，制定配套法律法规，系统、全面、总体性地进行数据安全治理体系建设，具有十分重要的意义，亦为本文研究的立足点。

从目前的研究成果来看，研究《数据安全法》与《网络安全法》《个人信息保护法》等相关法律之间的衔接与协调成为学者关注的热点。然而，图情档学者在数据安全相关法律的协调研究中参与不足，鲜有探讨《数据安全法》与《中华人民公共图书馆法》《中华人民共和国国家情报法》《档案法》等法律协调的研究成果。因此，文章试图通过对《数据安全法》和《档案法》进行协调研究，基于两部法律协调发展的内在逻辑与现实困境，探讨两者在"数据保护""重要数据的分级分类""档案与数据跨境流动"以及"个人数据的隐私保护"等问题上的协调，以期为图情档等领域立法与数据立法之间的衔接与协调提供借鉴，对档案与数据后续立法和管理实践开展有所启示。



## 2 《数据安全法》与《档案法》协调的内在逻辑

厘清"数据"与"档案"的法理概念交叉，剖析《数据安全法》与《档案法》在立法目的和立法原则上的异同协调，分析《数据安全法》与《档案法》的双向推动，是协调两部法律，完善配套下位法制定的逻辑起点。

### 2.1 两部法律规范的对象存在交叉与联系

从"数据"与"档案"的法律概念来看，两部法律规制的对象存在交叉与联系。相较于《网络安全法》将"网络数据"定义为"通过网络收集、存储、传输、处理和产生的各种电子数据"，《数据安全法》将"数据"定义为"任何以电子或者其他方式对信息的记录"，这便在形式上将纸质的档案信息以及其他书面形式对信息所作的记录也纳入数据范畴[15]。《档案法》将"档案"定义为"过去和现在的机关、团体、企业事业单位和其他组织以及个人从事经济、政治、文化、社会、生态文明、军事、外事、科技等方面活动直接形成的对国家和社会具有保存价值的各种文字、图表、声像等不同形式的历史记录"。同时，法国、英国、美国、加拿大等国家，均强调"档案"这个概念不受存在形式（时间、形式、载体等）影响，如表1所示：

表1 国外档案立法对"档案"概念的表述

| 国别 | 档案立法 | "档案"的定义 |
| --- | --- | --- |
| 法国 | 《遗产法典(第二卷:档案馆)》 | **第211-1条** 档案是所有自然人和法人，在其活动中产生或接收的，无论时间、保存地点、存在形式、载体形式的全部文件也包括数据的统称。 |
| 英国 | 《公共档案法》 | **第10条** "档案"不仅包括书面档案，也包括任何其他方式所承载的信息形成的档案。 |
| 美国 | 《档案处置法》 | **第3301条** 档案是指联邦机构根据联邦法律在处理公共事务过程中形成或接收的，以及作为美国政府组织、职能、政策、决策、程序、运作或其他活动的证据，或由于所含数据具有信息价值，而被联邦机构或其合法继任者保存或妥善保存的，各种载体形态或特征的所有记录信息。<br>"记录信息"一词包括所有的档案传统形式，无论其实体（物理）形式或特征，涵盖所有以数字或电子形式产生、处理、传递或存储的信息。 |
| 加拿大 | 《加拿大图书馆与档案馆法》 | **第2条** "档案"指的是任何媒介或者任何形式的文献材料，而不是出版物。 |

同时，大数据时代，档案管理实践从双轨制向单轨制、双套制向单套制的转轨，也将推动档案与数据立法的协调。《档案法》新增"档案信息化建设"一章，对档案数字资源的安全保存和有效利用作出针对性规定。其所称"档案数字资源"涵盖电子档案、传统载体档案数字化成果以及其他具有档案属性或档案价值的数字资源。也就是说，所有系统中生成的具有档案属性的数据，包括档案馆存储资源之外的数据资源，如政府公开数据、档案用户数据、社交媒体交互数据等都被看作是广义的档案[16]。因此，"数据"与"档案"在法律概念层面，均为广义上的"记录"，二者的涵盖范围互有交叉。档案与数据的概念内涵正相向而行，逐渐融合。

从产生主体和价值形态来看，二者的产生主体均包含机构、企业、个人，数据是有关部门、行业组织、企

业、个人开展数据活动时自然形成的“记录”,是业务开展的基础条件,强调即时性;档案是过去和现在的机关、团体、企业事业单位和其他组织以及个人形成的,是经过鉴定的、对国家和社会“具有保存价值”的“历史记录”,强调历时性。可以说,“档案”是经过鉴定的,对国家和社会具有长久保存价值的“数据”。同时,随着数字环境的蓬勃发展,档案与文件、信息、数据等的界限日渐模糊,许多信息载体如数据库、网页不能严格满足传统对于档案的定义,却具有较高的保存价值[17],“数据态”成为新的档案存在形态。

《数据安全法》着眼于数据处理活动与安全监管,也就是说,凡是进行数据处理活动的主体均需履行数据安全义务。同时,该法第五十三条第二款提出,在统计、档案工作中开展数据处理活动,开展涉及个人信息的数据处理活动,还应当遵守有关法律、行政法规的规定。既将《数据安全法》的适用范围扩大到档案部门这一负责“重要数据”长期保存的数据处理主体,也为《档案法》《中华人民共和国统计法》《个人信息保护法》等留出了立法接口和协调空间,明确了《档案法》在数据处理活动中的法律适用。

随着信息时代的到来,档案管理逐渐重视“业务前端数据的可保存性[18]”,对电子文件和电子档案提出的“全程管理”“前端控制”“来源可靠”管理要求与数据处理更重过程管理的理念不谋而合。相比于国家标准《信息安全技术 – 数据安全能力成熟度模型》(GB/T 37988 – 2019)将数据安全界定为“通过管理和技术措施,确保数据有效保护和合规使用的状态”,《数据安全法》从数据全生命周期角度出发,增加了“具有保障持续安全状态的能力”的数据管理要求,并提出“建立健全全流程数据安全管理制度”,体现出其对数据安全的认识从侧重过程安全渐趋注重长期安全。这一点与档案管理的目标具有内在联系。可以说,在“总体国家安全观”指导下,数据安全和档案安全的内涵和外延都突破传统安全观念,除了传统的“真实、完整、可用、安全”等共同要求外,还彼此借鉴吸纳了全程管理、前端控制、长期保存、风险控制等要求。

### 2.2 两者在立法目的和立法原则上各有侧重、相互补充

《档案法》与《数据安全法》的相继出台,是我国面对全球数据爆发增长和“存量数字化、增量电子化”的档案工作业态,对数据安全问题和档案管理现代化的立法回应。

在立法目的上,两者从数据处理和档案管理两个不同的向度,对数据安全管理活动做出规定,共同践行总体国家安全观的要求。《数据安全法》将数据安全提升到国家战略层级,其立法目的是“为了规范数据处理活动,保障数据安全,促进数据开发利用,保护个人、组织的合法权益,维护国家主权、安全和发展利益”。《数据安全法》所维护的数据安全是“通过采取必要措施,确保数据处于有效保护和合法利用的状态,以及具备保障持续安全状态的能力”,侧重现实的数据处理活动(数据的收集、存储、使用、加工、传输、提供、公开等)中的安全。《档案法》的立法目的包括“加强档案管理、提高档案信息化建设水平、为中国特色社会主义事业服务”三个方面。其对档案安全的要求主要是从实体安全和信息安全两个维度进行规定:档案实体安全指档案载体或存储介质的安全;档案信息安全是指档案的真实性、完整性、可靠性和安全性不受损害,档案开放利用过程中不违反相关的保密规定,不泄露档案信息[19]。此外,《档案法》更强调档案收集、整理、保护、利用及其监督等管理活动的规范化,以及档案实体和档案信息在永久或定期保存中的安全。

在立法原则上,两者在遵循《中华人民共和国立法法》所确定的基本立法原则的基础上,亦在保障安全与促进利用、权责一致等专业立法原则上达成共识。具体来说,《数据安全法》以保障数据安全与促进数据开发利用并重(第一、十三条)、数据安全工作协调治理(第五、六、九、十七、十八条)、权责一致(第四章数据安全保护义务)及维护数据主权(第一、二十五、二十六、三十六条等)[4]为立法原则。而经过 1987 年我国首部《档案法》出台以来三十余年的档案立法实践,《档案法》立法坚持中国共产党对档案工作的领导(第三条)、坚持档案工作统一领导、分级管理(第四条)、维护档案完整与安全(第一、四、十九、三十五条)、坚持档案利用权利与保护义务相统一(第一、四、五条)、坚持奖励与惩罚并行(第七、四十八、四十九、五十、五十一条)等原则。

### 2.3 《档案法》明确数据长期安全保存的具体要求

《档案法》对档案长期保存的安全管理要求与《数据安全法》对“具有保障持续安全状态的能力”的数据安全要求相契合。《档案法》对电子档案归档的法定要求以及实践中采取的备份、迁移、监控、日志管理、审计跟踪等档案数字资源长期保存措施,为规范数据处理流程、建立安全的数据处理模式,推动《数据安全法》与《档案法》协调进行数据全流程管控提供了借鉴。

截至2020年底,全国各级综合档案馆馆藏电子档案1 387.5TB,其中,数码照片390.2TB,数字录音、数字录像523.5TB。馆藏档案数字化成果19 588.5TB[20]。随着纸质档案数字化程度的不断提升,原生电子文件的数量加速增长,档案工作的对象正快速由“纸质档案”向“电子文件”(电子档案)转变。新修订《档案法》第三十七条规定电子档案应当“来源可靠、程序规范、要素合规”,从而保证电子档案的真实、完整、可用、安全;第三十九条提出对重要电子档案进行异地备份保管。备份的对象不仅包括电子档案本身,同时,基于电子档案数据恢复和有效利用的需求,还要备份元数据、电子档案管理信息系统配置文件与日志文件。这便从档案管理后端对数据管理系统软件、数据全过程全要素保存、数据处理全程管控、数据可理解可回溯等提出要求。

### 2.4 《数据安全法》为完善档案安全管理制度提供新思路

《数据安全法》从数据安全保护连贯性角度,为档案部门建立健全档案安全管理制度提供了新思路、新方向。《数据安全法》第三章“数据安全制度”涵盖数据分级分类保护(第二十一条)、数据安全风险评估(第二十二条)、数据安全应急处置(第二十三条)、数据安全审查(第二十四条)、数据出口管制(第二十五条)等各个环节,力图建立健全常态化、全流程的数据安全管理制度。档案安全是档案工作的生命线,在大数据时代更是面临着数据存储、档案传输、系统运维等非传统安全问题。然而《档案法》有关保障档案安全的规定,却散见于档案的管理、档案信息化建设、监督检查、法律责任各个章节,内容包括完善档案安全工作机制(第十九条)、保障档案实体安全(第十九条)、保障档案信息安全(第三十五条)、安全隐患补救(第四十四、四十五条)、严格法律责任(第四十八条),缺乏整体的原则、基础和连贯性。《数据安全法》有关数据安全风险监测评估、数据安全应急处置、数据安全的规定为完善档案安全管理制度提供了思路。

同时,《数据安全法》为档案部门获取数据管理“身份”提供了法律支撑。长期以来,档案部门在数据管理中时常处于“失语”和“缺席”的状态。档案部门作为重要数据的最终保存部门,数据治理顶层标准体系的建设直接影响到后续档案管理相关标准规范的制定,最终决定档案开发利用和安全保管的工作成效。《数据安全法》第五、六、九、十七、十八条等款项中有关建立国家数据安全工作协调机制、数据安全监管、推动相关行业组织制定数据安全行为规范、参与标准制定的规定,为档案部门参与数据安全协同治理提供了契机。

## 3 《数据安全法》与《档案法》协调的现存问题

当前,《数据安全法》和《档案法》两部法律均是从各自的管理实践出发,其前端数据处理与后端档案管理的制度连贯性不足,在档案与数据保护相关规定、档案与数据分级分类标准、档案与数据出境的监管主体等方面的法律规制协调性不足,容易造成数据的完整性、可用性、安全性得不到保障。

### 3.1 档案与数据保护相关规定不健全

档案安全是数据安全的重要组成部分,为数据的长期保存提供安全保障。目前,相比于《数据安全法》,《档案法》尚缺乏档案分级分类保护、档案安全风险监测评估预警、安全审查方面的具体规定,更加侧重于对安全隐患的后发性补救和不采取补救措施后的追责。同时,《档案法》的规制对象聚焦于档案本身的管理实践,缺乏对国家法制整体框架及数据管理或信息管理大环境等宏观背景的剖析和关切,容易导致学界和业界对档案部门参与数据安全协作治理的合法性认识不足。

就《数据安全法》而言,一方面,数据一旦被篡改、破坏、泄露或非法获取利用,将会对国家安全、公共利益或者组织、公民的合法权益造成极大危害。虽然《数据安全法》延续《网络安全法》的规定,对重要数据提出更高的数据保护要求,但数据安全负责人、管理机构、风险评估主体、报告报送对象、评估频率等有待后续立法进一步明确。另一方面,数据管理面临着系统漏洞、密码泄露、黑客攻击等挑战,数据存储的物理安全性和系统安全性要求越来越高,如何确保数据安全成为大数据时代数据管理的重要课题。《数据安全法》将数据处理的范围界定为数据的收集、存储、使用、加工、传输、提供、公开等。而与数据安全息息相关的数据“保护”,既是数据处理的终端活动,也是对数据处理全过程的要求,却未被纳入“数据处理”中,也未明确给出数据保护的具体责任归属。这便在法律的适用范围层面将数据“保护”排除在外,割裂了数据与档案、《数据安全法》与《档案法》之间的联系,易造成数据可靠性不足,电子档案的内容、结构和背景信息不齐全或丢失。

### 3.2 档案与数据分级分类标准不协调

从既有数据立法和档案立法来看，囿于不同的管理体系，档案和数据有着不同的分类方式。档案分类强调机构全宗，数据分类依据业务范畴[21]，并无必要苛求分类标准的统一。因此，本文从保障数据安全这一共识出发，从系统分级保护和内容分级保护两方面，探讨既有法律法规中数据和档案的分级标准，如表 2 所示：

表 2 既有法律法规有关档案/数据分级分类的规定

| 既有法律法规 | 具体款项内容 |
| --- | --- |
| 《数据安全法》 | **第二十一条** 国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。<br>关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。<br>各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。<br>**第二十七条** 开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。<br>重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。 |
| 档案领域相关法律法规 | **《中华人民共和国档案法实施办法》(尚未修订)第三条** 各级国家档案馆馆藏的永久保管档案分一、二、三级管理，分级的具体标准和管理办法由国家档案局制定。<br>**《档案信息系统安全等级保护定级工作指南》第 4 条** 档案信息系统是指开展档案业务所使用的档案信息管理系统、档案信息服务系统和档案办公系统等三类信息管理系统。<br>**第 5.2.3 条** 根据国家有关信息系统安全保护等级的相关规定和标准，从低到高依次划分为自主保护级、指导保护级、监督保护级、强制保护级、专控保护级五个安全等级。<br>**第 5.3.4 条** 确定档案信息系统安全保护等级时需要考虑业务信息安全和系统服务安全两个方面。 |

从系统分级保护来看，《数据安全法》第二十七条与《网络安全法》衔接，明确规定开展数据处理活动应当"在网络安全等级保护制度的基础上"，建立健全全流程安全管理制度，加强数据安全保护。在档案领域，目前档案信息系统定级保护亦处于《网络安全法》及其相关标准指南的规制下。《档案信息系统安全等级保护定级工作指南》编制参考的《信息安全技术 信息系统安全等级保护基本要求(GB/T 22239 – 2008)》《信息安全技术 信息系统安全等级保护定级指南》(GB/T 22240 – 2008)已在《网络安全法》出台的背景下，分别被《信息安全技术 网络安全等级保护基本要求(GB/T 22239 – 2019)》《信息安全技术 网络安全等级保护定级指南》(GB/T 22240 – 2020)代替。两个新标准将原"信息系统安全等级保护"的提法变更为"网络安全等级保护"，在定级对象、定级流程及方式、定级保护工作内容等方面进行了补充、细化和完善。而档案界尚未在新标准的基础上对《档案信息系统安全等级保护定级工作指南》进行修改，难以适应新的技术背景和法律法规对档案信息系统安全等级保护工作的要求。

从内容分级保护来看，《数据安全法》规定国家为建立数据分类分级保护制度的主体，为国家开展自上而下的监管提供了依据。同时，将重要数据更细粒度的具体目录和具体分类分级保护制度的制定权限下放到行业主管部门和各地区国家机关，由国家数据安全工作协调机制统筹协调，充分平衡了法律规定的普适性和灵活性。《档案法》对"有保存价值"档案的范围确定和"永久保管档案"分级标准、管理办法的制定，均由国家档案局自上而下开展，相较于《数据安全法》灵活性不足。同时，由于数据和档案处于不同的业务阶段，数据分级更多地基于对国家安全、公共利益或者个人、组织合法权益造成的危害程度等后果性标准，防止数据的非法获取、非法利用、篡改破坏泄露等，目的是在数据的现实开发利用过程中保护国家、公共、公民及组织的合法权益；档案分级是为了通过对档案进行价值鉴定，确定不同的保管期限和密级，重在对"历史记录"进行管理，确保其长期保存的安全。这便有可能导致在当下经济社会发展中具有重要价值的数据(如网络信息系统的缺陷、漏洞、防范措施、人群导航位置、大型设备目标位置和移动数据等)，可能并不会作为对国家和社会具有长久保存价值的档案保存下来。

### 3.3 档案与数据跨境流动规则不明晰

如表 3 所示，两部法律对数据与档案跨境流动的规定尚为概括性描述，监管主体不明晰。"重要数据"跨境流动是否允许档案部门参与管理，档案出境审批是否需要与数据管理部门协同共商，皆是当下亟需解决的问题。

虽然，《数据安全法》第三十一条与《网络安全法》

衔接，规定关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管

表3　两部法律有关数据与档案跨境流动的规定

| 法律法规名称 | 具体款项内容 |
| --- | --- |
| 《数据安全法》 | **第十一条** 国家积极开展数据安全治理、数据开发利用等领域的国际交流与合作，参与数据安全相关国际规则和标准的制定，促进数据跨境安全、自由流动。<br>**第二十五条** 国家对与维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制。<br>**第二十六条** 任何国家或者地区在与数据和数据开发利用技术等有关的投资、贸易等方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。<br>**第三十一条** 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。<br>**第三十六条** 中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供数据的请求。非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。 |
| 《档案法》 | **第二十五条** 属于国家所有的档案和本法第二十二条规定的档案及其复制件，禁止擅自运送、邮寄、携带出境或者通过互联网传输出境。确需出境的，按照国家有关规定办理审批手续。<br>**第五十条** 违反本法规定，擅自运送、邮寄、携带或者通过互联网传输禁止出境的档案或者其复制件出境的，由海关或者有关部门予以没收、阻断传输……并将没收、阻断传输的档案或者其复制件移交档案主管部门。 |

理，适用《网络安全法》的规定。但其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法有待进一步出台明确。同时，目前与重要数据出境相关的《个人信息和重要数据出境安全评估办法（征求意见稿）》《信息安全技术 数据出境安全评估指南（草案）》等相关具体规定仍处于征求意见稿或草案状态，且并未对涉及个人信息和重要数据的档案/数据跨境流动中的数据安全风险防控问题、参与数据安全国际规则与标准的具体层级或类别等作出具体规定，参考价值有限。

《档案法》对国家所有的，以及非国有企业、社会服务机构等单位和个人形成的对国家和社会具有重要保存价值或者应当保密的档案作出了严格的出境限制和法律责任的规定。在出境形式上，适应新载体档案的管理模式，将档案出境的形式扩展为运送、邮寄、携带出境和通过互联网传输出境[22]，涵盖了档案的实体出境和档案数据互联网传输出境。然而，上述规定仍停留在概括性表述，此前基于旧档案法的《中华人民共和国档案法实施办法》（以下简称《档案法实施办法》）以及2015年出台的《携带、运输、邮寄国家二级档案及其复制件出境审批事项服务指南》[23]等侧重实体档案出境，尚未根据新的数据传输方式和载体类型进行调整，可能因档案出境的监管和审批主体不明确，审查形式、标准及其流程不清晰，发生审查效率低下、行政审批不当、审查推诿等情况[13]。因此，亟需参考《数据安全法》《网络安全法》等相关立法，补充完善《档案法实施办法》等配套法律法规中有关档案出境的规定。

## 4 《数据安全法》与《档案法》协调的域外经验

面对数字时代信息技术和互联网的快速发展，大量产生的电子数据、信息和文件为档案管理工作实践带来了新的挑战。数据与档案的内生性联系逐渐体现在国外数据与档案相关立法实践中。国外档案与数据安全协调立法的经验能为我国《数据安全法》与《档案法》协调发展提供借鉴。

### 4.1 将数据安全二分为“网络安全”和“个人数据保护”

当前，全球数据保护立法多以“数据基本权利”为基础，将数据安全二分为网络安全和个人数据安全进行规制。2018年，欧盟颁布实施的《通用数据保护条例》（General Data Protection Regulation，GDPR）聚焦个人数据保护，对数据处理的原则、个人数据主体的权利、数据处理者和管理者的责任与义务、数据监管、数据跨境传输以及法律责任等方面作了详细且严格的规定。英国、德国、埃及以及印度等国家，总体上效仿欧盟《通用数据保护条例》的规定，对个人数据进行保护。2019年4月17日，欧洲议会和欧盟委员会颁布《网络安全法》（Cybersecurity Act，Regulation（EU）2019/881）[24]，对信息通信技术产品、服务和程序的安全提出要求，将重要数据的安全置于网络安全，特别是关键信息基础设施安全立法框架之下。

美国联邦层面并无统一的数据保护基本法，而是采取医疗、金融、教育等分领域立法[25]，各州也致力于制定自身的数据保护法规。联邦层面主要依据《通过

加强网络安全威胁信息共享提高美国的网络安全以及其他目的》(To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats and for other purposes)与《联邦信息安全管理法》《商业电子邮件信息法》《计算机安全法》等涉及网络安全的法律间接保护网络系统中的数据安全。2019年,美国国会研究服务局发布的《数据保护法:概述》(Data Protection Law:An Overview)认为,作为一个立法概念,"数据保护"融合了数据隐私和数据安全两大领域:前者包括控制个人数据的收集、使用等方面;后者包括如何保护个人数据免受未经授权的访问与使用,以及如何解决未经授权访问的问题等方面[26]。二者均指向个人数据。虽然2021年7月,美国统一法律委员会通过《统一个人数据保护法》(Uniform Personal Data Protection Act, UPDPA),旨在统一州隐私立法,但该法律目前尚未在美国各州立法机构通过,因此尚不具备法律效力。

值得注意的是,将数据安全二分为"网络安全"和"个人数据保护"的立法模式,虽未直接与档案立法衔接,却也能在一定程度上补充档案立法在管理系统安全、个人信息保护等方面的未尽之处。如2018年,英国修订并颁布的《数据保护法》(Data Protection Act 2018)对公民个人信息进行了全方位的保护,弥补了《公共档案法》《环境信息条例》和《信息自由法》在个人信息保护方面存在的不足,成为英国国家档案信息法律条例的重要组成部分[27]。美国《信息自由法》规定了信息公开与不公开的标准,赋予公众向联邦政府索取档案材料的权利。此外,《隐私权法》试图解决美国联邦机构进行政府信息公开与个人信息保护两种制度之间的矛盾,规定利用涉及普通公民的个人信息须经本人许可、确保信息用向合法合理。但总的来说,二分法模式下数据立法与档案立法之间的协调性仍然不足。

### 4.2 档案与数据融合立法的瑞士实践

1992年,瑞士联邦颁布《联邦数据保护法》(Loi fédérale sur la protection des données),旨在保护数据主体的人格和基本权利。其中第八条规定了档案管理员可提供访问的数据类别及提供访问的形式,第二十一条明确了《联邦档案法》在个人数据保护中的适用[28]。该法的出台标志着瑞士的档案工作不仅受《联邦档案法》的规制,同时受《联邦数据保护法》等一系列与档案工作有关的法律共同规制[29]。

2008年,瑞士阿尔高州颁布了《公共信息、数据保护和档案法》(Loi sur l' information du public, la protection des données et les archives),这是瑞士境内第一次将"公共信息""数据保护"和"档案工作"三个相关主题放在同一部立法中[29]。《公共信息、数据保护与档案法》的立法目的之一便是确保档案部门等公共机构在处理个人数据时尊重个人权利和基本自由。三个部分并非孤立地规制各自领域的管理活动,档案工作者在公共信息、数据、档案保护衔接中扮演了重要的协调作用,同时第6章"程序规定和法律补救措施"以及第7章"最后和过渡性条款"等对三者的协调对接做出补充说明。

大数据时代,瑞士联邦档案馆采用关联数据技术,对联邦政府、州和市政当局等不同来源的结构化数据进行跨组织集成和关联,提供关联数据服务(LINDAS)[30]。这种"关联数据服务"打破了从数据到档案的线性管理流程,优化并提高了档案与数据的利用方式和效率。瑞士将档案与数据融合立法,既为数据提供者扫除了数据权属问题的担忧,为数据生成部门和档案部门协同进行数据治理、信息资源开发利用奠定了法律基础,又将档案部门纳入数据安全保护中,能够在立法层面减少重复立法和法律冲突,降低立法成本。同时,能够在实践层面有效保障"数据保护"和"档案管理"活动的协调与融合,增强数据治理连贯性,促进数据开发利用。

### 4.3 国际组织对档案与数据协调立法的引导

2018年10月,欧洲档案联盟(The European Archive Group, EAG)颁布《档案服务数据保护指南》(Guidance on data protection for archives services),作为档案部门落实《通用数据保护条例》的指南,内容包括处理个人数据的一般原则、什么是"出于公共利益的归档"、数据主体的权利、需要特殊保障措施的个人数据类别、数据安全、提高透明度和促进遵约的措施等[31],为国家档案馆、博物馆、图书馆和其他保存档案的公共和私营机构应用《通用数据保护条例》提供实用指南,为档案部门、档案工作人员进行个人数据保护提供指导。2020年3月,国际档案理事会(ICA)与国际图书馆协会联合会(IFLA)联合发表的《关于隐私立法与存档的声明(草案)》(IFLA-ICA Statement on Privacy Legislation and Archiving)认为档案中不可避免地含有个人身份信息,并从档案的角度提出了一些有关个人数据保护立法的建议,旨在为图书馆、档案馆及其协会在倡导数据保护法律方面制定核心原则[32]。可见,国际组织对于档案部门在数据安全保护中的参与也主要集

中在个人数据方面。

无论是瑞士的档案与数据融合立法，还是国际组织对档案与数据协调立法的引导，均更加侧重档案部门在“个人数据”安全保护中的参与。我国的《数据安全法》作为一部兼具个人、公共、国家三个面向的数据保护法律[33]，在数据的概念范畴、适用范围、数据安全制度的制定、各类数据活动开展等各个方面，需要考虑不同部门、不同行业、不同企业，乃至不同国家的数据管理诉求，在具体条文上面临着与《中华人民共和国保密法》《网络安全法》《档案法》《个人信息保护法》等法律法规相衔接的问题。特别是在与《档案法》的协调中，除了借鉴国外经验，明确档案部门在个人数据安全保护中的参与，两部法律后续配套法律法规的制定还均需在数据保护、重要数据的分级分类保护、个人隐私保护、数据跨境流动等方面进行完善和协调。

## 5 《数据安全法》与《档案法》协调的对策建议

面对上述《数据安全法》与《档案法》协调发展的内在逻辑和现存困境，以及大数据时代对档案与数据安全治理提出的新要求，研究从统筹协调数据全生命周期管理相关法律法规、建立健全数据安全协作机制的角度，对《数据安全法》和《档案法》后续法律法规的完善提出建议。

### 5.1 明确档案部门在数据安全协作机制中的参与

《数据安全法》第五、六、九、十七、十八条等多个款项提出建立数据安全工作协调机制，推动有关部门参与数据安全保护工作，在数据安全风险评估、防范、处置等方面开展协作。考虑到数据管理与档案管理对象的重叠、档案部门和数据管理部门职能的交叉，应推动档案部门与数据管理部门之间职能的协调优化[8]，使档案部门融入数据安全协同治理体系，获得数据管理身份，以便在数据开发利用和数据安全标准体系建设层面，从数据后端管理视角，提出建议、发出声音，反驱数据开发利用和数据安全标准的完善。

具体来说，一方面，基于数据安全协作机制明确档案部门在数据治理中的席位。应以《数据安全法》《个人信息保护法》的出台为契机，统筹考虑档案部门、数据管理部门、文件管理部门、政府信息公开主管部门、保密行政管理等有关部门的职能关系，增补国家档案局为促进大数据发展部际联席会议成员单位。从国家、地方、机构各个层面推动档案部门加入协作式数据治理组织，落实数据安全协同治理体系中的档案参与。另一方面，在“国家电子文件管理部际联席会议”的组织架构基础上，推动数据管理部门参与电子档案协同治理机制，以适应档案信息化及《档案法》对电子档案的管理要求。从而实现档案部门与其他数据管理部门的双向合作，既推动档案部门参与大数据时代的数据协同治理，也通过与其他数据管理部门的共同努力推动档案管理在法治轨道上行稳致远。

此外，《数据安全法》第十七条提出，“国家推进数据开发利用技术和数据安全标准体系建设。国务院标准化行政主管部门和国务院有关部门根据各自的职责，组织制定并适时修订有关数据开发利用技术、产品和数据安全相关标准……”，档案部门可积极参与其中，从数据长期保存有效利用的角度建言献策，同时推动《档案馆安全风险评估指标体系》《档案信息系统安全保护基本要求》《档案数字化外包安全管理规范》等相关规范性文件的及时更新。

### 5.2 建立符合我国实践的数据与档案分级分类标准

一方面，“数据”与“档案”的有机联系决定了部分重要数据最终将进入档案馆，“重要数据”的长期保存和安全，能够为“重要数据”的归档管理奠定前端控制的质量基础。目前数据分级分类和档案分级分类的不协调、数据价值和档案价值鉴定标准的不衔接，易导致部分数据陷入进退两难的“灰色地带”（即档案部门认为对国家和社会具有长久保存价值的数据未被归为“重要数据”进行保护；数据管理部门归为的“重要数据”未进行归档保存），从而导致这部分数据的真实性、完整性、可用性、安全性不足。有学者从数据作为执政资源的角度提出，建立数据分级分类目录及重要数据目录，在做好内部数据治理的基础上，根据国家、主管部门、行业重要数据具体目录建立或细化相对应的数据保护目录和制度，匹配数据分类分级保护制度的监管要求[34]。因此，后续《数据安全法》配套法律法规应将档案部门纳入“数据分级分类”及“重要数据目录”的确定主体中，推动档案部门参与后续重要数据分类、出境管理等相关法律法规的制定。

另一方面，档案部门应同数据管理部门以及相关行业机构共商档案分级保护机制，制定符合我国基本国情和档案管理实践的档案分级标准。此前，已有学者在《网络安全法》将等级保护工作提升到法律层面的背景下，研究了如何在我国网络安全等级保护2.0体系要求下做好档案网络安全等级保护工作[35]。《“十四五”全国档案事业发展规划》提出要完善档案

法规制度和标准规范,做好新修订档案法配套法规、规章、行政规范性文件的立改废释工作……及时修订、清理与现实需要不相适应的法规、规章和行政规范性文件。因此,后续《档案法实施办法》等配套下位法的制定应与《档案法》《数据安全法》《网络安全法》《信息安全等级保护管理办法》《信息安全技术、信息系统安全等级保护基本要求》《工业数据分类分级指南(试行)》等指引性文件及行业标准相承接,不仅要基于各自领域的保存需求和管理困境,更要从数字信息的安全保存有效利用的连贯性来考虑。具体来说,可借鉴《数据安全法》对数据在经济社会发展中重要程度的关注,根据档案的重要程度、保密程度、敏感程度、现实利用需求,结合实际管理需求划分出不同的安全级别,对档案实行针对性、多层次的安全保护[12]。同时,及时根据网络安全等级保护的新指南新标准,更新档案信息系统分级保护相关标准。

### 5.3 完善数据与档案跨境流动的法律规制

在数字经济蓬勃发展的时代背景之下,数据跨境流动成为新常态[36]。我国《大数据产业发展规划(2016-2020年)》明确提出要"推动建立数据跨境流动的法律体系和管理机制,加强重要敏感数据跨境流动的管理"。《数据安全法》第十一条提出数据跨境流动的基本原则——安全自由流动,将"数据自由流动"作为基础性原则,将"数据安全流动"作为限制性原则,以平衡对外开放和国家安全的双重目标,为全球数据治理提供了审慎包容、鼓励合作的中国方案[37]。数据跨境流动对数据安全的考察,静态上体现为对数据原有形态及其权利的保护,动态上体现为流动过程的合法、可信、可控[38]。虽然《数据安全法》第二十五条、第三十条、第三十六条等对数据出口管制、重要数据出境安全管理、向外国司法或执法机构提供数据等事项均作出了法律规制。然而目前,数据跨境流动仍面临数据分级分类制度不健全、监管手段缺乏灵活性等困难和挑战[39]。一方面,《数据安全法》缺少具体的分类分级标准和法律责任条款,另一方面,如前文所述,目前数据分级分类和档案分级分类的不协调,易导致部分数据的监管主体不明。因此,后续《数据安全法》配套法律法规的制定应与《档案法》协调,在档案部门参与确定重要数据、数据分级分类标准的基础上,确保数据跨境流动中的完整、保密、可用、安全。

目前,《档案法》主要对国有档案和第二十二条规定的档案及其复制件的出境审批作出了规制。而档案出境引发的档案安全风险,体现在档案的传输、存储和应用等各个环节,贯穿于出境前、出境中、出境后各个时期。基于此,档案部门可依据《数据安全法》第三十一条的规定,积极参与重要数据出境安全管理办法制定。后续《档案法实施办法》等档案法规的制定亦需在重要档案目录确定、出境档案限制清单、档案出境审批流程、出境档案监管主体、违规出境处罚等方面与《数据安全法》协调对接。同时,档案出境时,应严格遵循审核流程,办理审批手续,进行数据安全评估、内容审核、数据脱敏、建立档案出境记录。此外,档案出境后,既要熟悉所在国家或地区档案法律规定并严格遵守[40],如俄罗斯对"本地强制储存"的要求[41],同时也要借鉴《数据安全法》第二条和第二十六条对法律域外适用和反制裁措施的规定,提升《档案法》的域外适用性。总的来说,档案跨境流动不仅涉及档案出境,也包括档案入境。我国《档案法》后续下位法的制定,既要与我国既有《数据安全法》《网络安全法》《个人信息保护法》等相关数据立法相协调,也要剖析体认国际上有关数据跨境流动的标准规范(如美国的《澄清境外合法使用数据法案》、欧盟的《通用数据保护条例》以及经济合作与发展组织的《关于保护隐私与个人数据跨境流动的指南的建议》)中存在的问题,积极参与档案跨境流动国际标准规则的制定和公约的签订,进而维护我国的数据主权。

### 5.4 完善两部法律有关个人隐私保护的内容

2021年8月20日,第十三届全国人民代表大会常务委员会第三十次会议通过《个人信息保护法》,对个人信息处理活动作出法律规制。而目前来看,我国《数据安全法》《档案法》等将个人信息、个人隐私、商业秘密一并予以列举,这种概念范围的重复和交叉,增加了法律使用中辨析两个概念的难度。后续档案立法还需与《中华人民共和国民法典》(以下简称《民法典》)《个人信息保护法》协调,理清个人信息保护与个人隐私保护的边界。

对于规范数据处理活动来说,一方面,《数据安全法》后续配套下位法的制定中,须明确开展数据处理活动损害个人合法权益时的适用法律,从而与《民法典》《中华人民共和国侵权责任法》《网络安全法》《个人信息保护法》《档案法》等法律法规协调衔接,构建整体的隐私保护法制环境。另一方面,可借鉴瑞士阿尔高州《公共信息、数据保护和档案法》,在《数据安全法》配套法律法规的制定中,增加对未经授权的个人数据访问、使用、披露、破坏、修改或销毁等行为的风险控制措施和救济条款,建立大数据时代个人隐私侵权的预

防、监测和救济机制,补充数据空间的个人隐私保护立法。

对于档案管理活动来说,后续《档案法实施办法》等下位法的修订可借鉴国外个人数据保护立法的经验,与《民法典》《个人信息保护法》《数据安全法》《网络安全法》《档案法》等相关法律法规对接协调,补充《档案法》中有关个人隐私信息保护的内容。如《关于隐私立法与存档的声明(草案)》提出的建立有关档案中的个人身份信息的访问机制、健全相关记录管理和档案规划,需要图书馆和档案馆工作者基于伦理原则做出专业判断,进行相应的访问限制[32]。此外,可借鉴澳大利亚新南威尔士州信息和隐私委员会推出的"隐私治理框架"(Privacy Governance Framework)[42],与其他数据管理部门协作推出个人隐私数据治理框架、个人数据出境隐私风险评估等工具,以便在档案收集、开放共享、公布利用、出境审核等工作环节中,应对各种黑客程序、网络病毒、蓄意侵权等行为给个人隐私保护带来的挑战,对档案中的个人隐私和档案用户的隐私进行保护。

## 6 结语

无论是《数据安全法》,还是《档案法》,法律的制定只是开始,加强相关法律、新旧政策、具体实践之间的统筹协调,才是保障数据安全,进行数据治理的题中之义。本文对《数据安全法》与《档案法》协调发展的动力源泉进行了双向审视,提出由于当前《数据安全法》与《档案法》主要是从各自的管理实践出发,法律间协调性不足,导致部分数据无人在管、无法可依,数据的长期保存、有效利用、完整安全无从保证。由此指出应将档案部门在数据治理中的参与、数据与档案分级分类标准的协调、数据与档案跨境流动中的安全保护、个人隐私保护等问题融入《数据安全法》与《档案法》配套法规、规章、行政规范性文件的立改废释中。同时,当下档案与数据管理职能划分仍存在争议,档案部门如何与数据管理部门协同进行数据治理仍言犹未尽,配套制度的完善和健全、档案管理思维与数据管理思维的相互融合也有待进一步深入研究探讨。



**参考文献:**

[1] 审时度势精心谋划超前布局力争主动 实施国家大数据战略加快建设数字中国[N]. 人民日报,2017-12-10(001).
[2] 翟志勇. 数据安全法的体系定位[J]. 苏州大学学报(哲学社会科学版),2021,42(1):73-83.
[3] 张猛. 数据安全法草案与网络安全法部分条款的对比评析[J]. 网络安全和信息化,2020(10):25-26.
[4] 刘桂锋,阮冰颖,刘琼. 加强数据安全防护 提升数据治理能力——《中华人民共和国数据安全法(草案)》解读[J]. 农业图书情报学报,2021,33(4):4-13.
[5] 马忠法,胡玲. 论我国数据安全保护法律制度的完善[J]. 科技与法律(中英文),2021,(2):1-7,75.
[6] 徐玖玖. 数据法治安全与发展价值的衡平路径——以《数据安全法(草案)》的突破与困境为视角[J]. 山东科技大学学报(社会科学版),2021,23(2):38-43,61.
[7] 赵生辉,胡莹."档案数据化"底层逻辑的解析与启示[J]. 档案学通讯,2021(4):20-27.
[8] 刘越男. 数据治理:大数据时代档案管理的新视角和新职能[J]. 档案学研究,2020(5):50-57.
[9] 赵生辉,胡莹. 拥有整体性记忆:档案领域数据本体管理论纲[J]. 山西档案,2020(6):17-27.
[10] 中国人民大学未来法治研究院. 建立完善数据安全法律体系[N]. 经济参考报,2020-09-15(008).
[11] 邓灵斌.《数据安全法(草案)》解读及我国图书情报界的对策建议[J]. 情报杂志,2020,39(12):83-87.
[12] 金波,杨鹏. 大数据时代档案数据安全治理策略探析[J]. 情报科学,2020,38(9):30-35.
[13] 耿志杰,刘志森. 档案数据互联网传输出境的实施困境与完善策略[J]. 浙江档案,2021(3):24-26.
[14] 丁家友,周涵潇,张照余. 数据安全与档案事业高质量发展——《"十四五"全国档案事业发展规划》解读与思考[J]. 档案与建设,2021(9):12-15,11.
[15] 吴卫明,吴俐. 全面信息安全与数据合理利用——简评《数据安全法(草案)》[J]. 信息安全与通信保密,2020(8):23-28.
[16] 王协舟,王露露."互联网+"时代对档案工作的挑战[J]. 档案学研究,2016(6):66-69.
[17] 徐拥军,李孟秋. 数字连续性战略视域下的档案管理体制改革[J]. 档案与建设,2020(5):4-10.
[18] 钱毅. 数据态环境中数字档案对象保存问题与策略分析[J]. 档案学通讯,2019(4):40-47.
[19] 王英玮,杨千. 总体国家安全观视角下《中华人民共和国档案法》的安全理念[J]. 档案学研究,2020(6):78-85.
[20] 中华人民共和国国家档案局. 2020 年度全国档案主管部门和档案馆基本情况摘要(二)[EB/OL]. (2021-08-06)[2021-08-27]. https://www.saac.gov.cn/daj/zhdt/202108/6262a796fdc3487d93bfa7005acfe2ae.shtml.
[21] 陈兴跃. 数据分级分类正式入法具有重大实践指导意义[J]. 信息安全研究,2020,6(10):949-952.
[22] 国家档案局政策法规研究司. 新修订的《中华人民共和国档案法》解读[J]. 中国档案,2020(7):24-25.
[23] 国家档案局政策法规司. 携带、运输、邮寄国家二级档案及其复制件出境的审批[EB/OL]. [2021-04-16]. https://www.saac.gov.cn/daj/xzsp/201509/5b499a02ce9f495baec0c8288b5abede.shtml.
[24] OFFICIAL JOURNAL OF THE EUROPEAN UNION. Regulation (EU) 2019/881 of the European parliament and of the council [EB/OL]. (2019-04-17)[2021-04-27]. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&qid=1619490925226&from=EN.

[25] 龙卫球. 数据新型财产权构建及其体系研究[J]. 政法论坛,2017,35(4):63-77.
[26] 张臻,李艳. 美国《数据保护法概况》报告述评[J]. 保密科学技术,2019(8):29-35.
[27] 曹宇,赖文渊. 英国国家档案法律体系概述[J]. 辽宁大学学报(哲学社会科学版), 2011,39(5):79-86.
[28] THE PUBLICATION PLATFORM FOR FEDERAL LAW. Loi fédérale du 19 juin 1992 sur la protection des données (LPD)[EB/OL]. [2021-05-09]. https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/fr.
[29] 国家档案局政策法规研究司. 境外国家和地区档案法律法规选编[M]. 北京:中国政法大学出版社,2017.
[30] 王志宇,王晓宇. 瑞士联邦档案馆特色功能研究及启示[J]. 北京档案,2021(5):40-43.
[31] EUROPEAN ARCHIVE GROUP. Guidance on data protection for archives services[EB/OL]. [2020-07-15]. https://ec.europa.eu/info/sites/info/files/eag_draft_guidelines_1_11_0.pdf.
[32] INTERNATIONAL COUNCIL ON ARCHIVES. IFLA-ICA statement on privacy legislation and archiving[EB/OL]. [2020-07-26]. https://www.ica.org/sites/default/files/privacy_legislation_and_archiving_statement_chinese.pdf.
[33] 黄道丽,胡文华. 中国数据安全立法形势、困境与对策——兼评《数据安全法(草案)》[J]. 北京航空航天大学学报(社会科学版),2020,33(6):9-17.
[34] 欧黎. 坚持党管数据 保障数据安全[J]. 旗帜,2021(8):45-46.
[35] 郑川,曹阳,向禹,等. 新形势下档案网络安全等级保护:变化与对策[J]. 山西档案,2021(2):25-34.
[36] 杨署东,谢卓君. 跨境数据流动贸易规制之例外条款:定位、范式与反思[J/OL]. 重庆大学学报(社会科学版):1-15[2021-08-30]. http://kns.cnki.net/kcms/detail/50.1023.C.20210826.1451.002.html.
[37] 许可. 自由与安全:数据跨境流动的中国方案[J]. 环球法律评论,2021,43(1):22-37.
[38] 黄现清. 数字贸易背景下我国数据跨境流动监管规则的构建路径[J]. 西南金融,2021(8):74-84.
[39] 王志杰. 论我国跨境数据流动的监管完善——基于数据安全性与数据开放性的利益平衡视角[J]. 福建金融,2021(7):9-16.
[40] 徐拥军,舒蓉,李孟秋. 我国企业境外档案管理面临的法律冲突与适用原则[J]. 档案学通讯,2018(4):9-14.
[41] 何波. 俄罗斯跨境数据流动立法规则与执法实践[J]. 大数据,2016,2(6):129-134.
[42] INFORMATION AND PRIVACY COMMISSION. Privacy governance framework[EB/OL]. [2021-04-16]. https://www.ipc.nsw.gov.au/privacy/agencies/privacy-governance-framework.

**作者贡献说明:**
王玉珏:提出论文选题、设计论文结构、指导与修改论文;
吴一诺:收集资料、组织与撰写论文、修改论文;
凌敏菡:收集资料、撰写初稿。

## Study on the Harmonization of *Data Security Law* with *Archives Law*

Wang Yujue[1] Wu Yinuo[1,2] Ling Minhan[1]
[1] School of Information Management, Wuhan University, WuHan 430072
[2] National Demonstration Center for Experimental Library and Information Science Education, Wuhan University, WuHan 430072

Abstract: [**Purpose/significance**] By analyzing the respective emphasis and overlap between the *Data Security Law* and the *Archives Law* in terms of regulatory objects, legislative purposes and legislative principles, this paper explores the necessity and possible paths to promote the coordinated development of two laws, and is to provide references for the follow-up legislation on archives and data. [**Method/process**] Through literature research and comparative analysis, this paper put forward the main problems in the process of coordinated development of two laws, and made suggestions on the formulation of the supporting subordinate laws of two laws through foreign experience. [**Result/conclusion**] This study finds, starting from their respective management practices, the two laws lack the coordination of legal regulations in the relevant provisions of archives and data protection, the classification standards of archives and data and the cross-border flow of archives and data, resulting in some data falling into a "gray area" and no guarantee of data security. The paper proposes that the participation of the archives department in data governance should be clarified; based on the consistency of long-term data preservation, establishing the classification standards of archives and data corresponding to our country's actual conditions; the archives department and the data department should coordinate to establish laws, regulations and management mechanisms for the cross-border flow of important data; improving the content of personal privacy protection in two laws.

Keywords: *Data Security Law* *Archives Law* data security archives legislation data legislation